4. TCP ACK scans: When you knock on the firewall's door just to see who yells back!

The `TCP ACK` scan is a network probing technique used primarily to determine the filtering rules of a firewall. By sending a packet with the `ACK` flag set to various ports, and observing whether the target responds with an `RST` packet, security professionals can infer whether ports are statefully inspected.

You are a network administrator responsible for verifying the firewall rules for a newly deployed section of your corporate network. Before deploying critical services, you want to ensure that the firewall is properly filtering unexpected external ACK packets, which should all be blocked or filtered to enhance security against potential reconnaissance activities by attackers.

Write a bash script that performs a TCP ACK scan on a specified test network. The scan should identify potential stealth ports, focusing on ports `80`, `22`, `25`.

- Your script should accept `host` as an arguments `$1`.
- Your script should accept `ports` as an arguments `$2`.
- Your script should display the reason each port is set to a specific state.
- Your script should enforce a time limit of `1000` milliseconds for each host response.

Depending on the scanned network, the output could change.

```
┌──(maroua)-[~/0x06_nmap_advanced_port_scans]
└─⚑  ./4-ask_scan.sh www.holbertonschool.com 80,22,25
[sudo] password for maroua:
Starting Nmap 7.80 ( https://nmap.org ) at 2024-04-19 13:28 CET
Nmap scan report for www.holbertonschool.com (52.17.119.105)
Host is up, received reset ttl 31 (0.17s latency).
Other addresses for www.holbertonschool.com (not scanned): 63.35.51.142
34.249.200.254 64:ff9b::3f23:338e 64:ff9b::3411:7769 64:ff9b::22f9:c8fe
rDNS record for 52.17.119.105: ec2-52-17-119-105.eu-west-
1.compute.amazonaws.com

PORT   STATE      SERVICE REASON
22/tcp unfiltered ssh     reset ttl 20
25/tcp unfiltered smtp    reset ttl 18
80/tcp unfiltered http    reset ttl 27

Nmap done: 1 IP address (1 host up) scanned in 0.57 seconds
```